- Blog
- Resources
- Careers
- Developers
- Contact TeleSign
- Customer Login

Toggle navigation

- Home
- Mobile Identity
- Solutions
- Customers
- Partners
- Company
- Blog
- Careers
- Developers
- Contact TeleSign
- Customer Login

# TeleSign Introduces REST APIs

In Announcements - Feb 21, 2012

One of the things TeleSign is working on in Q1 is making our APIs available via a REST interface. Today all of our customers access our APIs via SOAP and we’ve definitely heard that folks want us to provide our APIs in an alternative form since almost all Web Services today use REST.

When developing this API we wanted to make sure we were using best practices from a security perspective and that we were developing the API in a way that would be familiar and easy to implement for developers. Unlike SOAP, which has a specific protocol specification around the exchanging of structured information that can be used to create Web Services or other types of services, REST refers to a general software architecture and this architecture can then be used to create web services. In creating a RESTful API the developer then uses things like RFCs and other web standards to create the interface.

When creating the API one of our key goals other than making the API easy to use, extensible and highly performant was to use the very best practices in securing the interface. To be as secure as possible we’ve implemented HMAC (Hash-based Message Authentication Code) in our auth process to ensure that both communications are properly authenticated and that they can’t be manipulated in transit.

To make HMAC work the first thing we do is allow users to share a secret with us. In this case the secret API-Key is generated automatically by TeleSign (to ensure that the key is truly random and not guessable) and then this key is given to the user in our web portal. In the new web portal users will be able to define expiration times for their keys and even be able to generate multiple keys so that they can rotate their keys with us.

The basic way HMAC authentication works is:

1. The sender and recipient share a secret, for this blog let’s just call the secret “The API Key” (an API key is just a randomly generated password like “mRW1Q8xDYTPc423YJs12Aeqk0nPGrtO5“)
2. The sender when they send their request includes an “Authorization” header with the following attributes:

There are a few advantages to this method:

1. The secret information is never passed between each party during the transaciton.
2. Because each party has a copy of the secret key, the sender and recipient are independently able to create the “Authoirzation” token. As long as the token is created in the same way on each side the authorization of the transaction will succeed.
3. Because the authorization token contains a hash of not only th API Key but the transaction as well, the recipient can be assured that both the transaction is properly authenticated and that it hasn't been modified in transit.

There are two additional items in our HMAC authentication that also offer security to the transaction:

1. The inclusion of “Date” in the string to sign.
2. The option of adding a cryptographic nonce to the header.

The advantage of adding a “Date” to the signature string is that it limits the time frame, in which, if somehow a transaction is captured between the sender and recipient that that transaction can be replayed. While all communication between the sender and the recipient will be over SSL, it’s always possible that there is some compromise in the sender’s infrastructure such that data is captured before it is sent over the SSL channel. In this case the addition of Date allows TeleSign to define a window where we will only accept transactions for a given defined Date within a certain window.

The other thing we do to make sure that transaction can’t be replayed is provide the customer the option to include a cryptographic nonce in the transaction. With a nonce included in the hash and passed to us as a header we can store the nonce for a set period of time that is the same as the Date window described above. Using the nonce even if a transaction is captured and the attacker is able to replay that transaction in the Date window, that transaction will only be good once if a nonce is included. If we see a duplicate transaction in a Date window with a duplicate nonce we’ll know that the transaction is a bogus one and alarm bells will go off.

To learn more about the use of HMAC you can read a very good article on Wikipedia here or you can read RFC 2104. To learn more about cryptographic nonces you can read more here.

**Share**

## Related Posts

# TeleSign Named a Leader in 2014 Magic Quadrant

Gartner recently released the Magic Quadrant for User Authentication and has named TeleSign a leader in the space. This Magic …

**Published in:** Announcements

## TeleSign Infrastructure Not Vulnerable to Heartbleed

TeleSign's operations and engineering team has conducted a comprehensive security audit of our systems confirming that we were not susceptible to the Heartbleed vulnerability. As should anyone who provides a Internet service, our audit involved a review of all systems and devices that utilize the OpenSSL library for SSL communications.

**Published in:** Announcements

heartbleed

## Employee Spotlight: Mei Chen

TeleSign's Employee Spotlight profiles some of the people and projects that make TeleSign a success.

**Published in:** Announcements

View All Blog Posts

Search for:

Search the blog...

Your email:

Enter your email address... Subscribe

## Topics

- Announcements
- Product Highlights
- Threats & Trends

## Featured Posts

How TeleSign Helps Citrix ShareFile Provide Additional Security to Global Users

TeleSign AuthID Kit – Helping Developers Remove the Cost Barriers and Complexities of Authentication

How Evernote Protects Global Accounts From Compromise With TeleSign

TeleSign Named a Leader in 2014 Magic Quadrant

TeleSign Helps Salesforce Keep Millions of Customers Secure With Mobile Verification

Tinder Reduces Spam Traffic 90 Percent With TeleSign

## Solutions

- Account Registration
- Account Access and Usage
- Account Recovery

## Products

- SMS & Voice Verification
- Mobile App-Based Authentication
- PhoneID Fraud Prevention

## About

- Mobile Identity
- Company
- Careers
- Customers
- Partners

## Resources

- Blog
- Case Studies
- Datasheets
- eGuides
- Events
- Newsroom
- Videos
- Webinars

“TeleSign worked closely with us to ensure our user interface and user experience provided the best experience possible and would be easily adopted.” - Dave Engberg, CTO @ Evernote

Get Started Now

**Los Angeles Headquarters**
4136 Del Rey Avenue
Marina del Rey, CA 90292- USA
Direct Dial: +1 310 740 9700
Toll Free: 1 800 850 3485

- /Terms & Conditions
- /Privacy Notice